BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-104

23 APRIL 2012

Intelligence

OVERSIGHT OF INTELLIGENCE ACTIVITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: AF/A2RP
Supersedes: AFI 14-104, 16 April 2007

Certified by: AF/A2Z
(Mr. Joseph D. Yount)
Pages: 30

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations* and is consistent with Executive Order (EO) 12333 (part 2), *United States Intelligence Activities*; Department of Defense (DoD) Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*; DoD Directive, and (DoDD) 5240.1, *DoD Intelligence Activities.* This publication states the requirements for United States Air Force intelligence oversight activities. In this publication, the term intelligence refers to intelligence and counterintelligence units, activities, etc. It describes mandatory intelligence oversight-associated training requirements for Air Force components that conduct intelligence activities. It also details how to identify, investigate, and report in the event of possible violations. This publication does not apply to criminal investigative activities. For purposes of this publication, the National Guard Bureau is a MAJCOM. This instruction applies to all Air Force (USAF), Air Force Reserve (USAFR) and Air National Guard (ANG) [in Title 10 or Title 32 (U.S.C.) status when assigned or attached to intelligence units or staffs]; and civilian personnel including, but not limited to, civil service, contract and Host Nation employees engaged in or performing intelligence-related activities as provided for in paragraph 2. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**/. Send recommended changes using the AF Form 847, *Recommendation for Change of Publication* to AF/A2 Policy workflow via NIPR or SIPRnet. This publication may be supplemented at any level, but all direct Supplements must be routed through the OPR prior to certification and approval to AF/A2 Policy workflow via NIPR or SIPRnet.

SUMMARY OF CHANGES

This publication is substantially revised and must be completely reviewed. It adds reporting requirements, if required, of verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters to the United States Attorney General. This revision updates standards for initial, annual, and pre-deployment training, IO program inspection guidance as well as unit self-inspection criteria. It clarifies undisclosed participation of personnel assigned to the AF ISR Agency for foreign intelligence purposes as well as senior leader training requirements. It updates annual and quarterly IO reporting procedures. It adds AF/JA as a voting member of the IO Panel, and also adds AF/JA to the list of offices required to coordinate on quarterly and annual IO reports. It creates Proper Use Memorandum (PUM) guidance for airborne platforms. References and definitions have been substantially updated.

1. Purpose. Intelligence oversight (IO) involves a balancing of two fundamental interests: obtaining the intelligence information required to protect national security and protecting individual rights guaranteed by the Constitution and the laws of the United States (US). The primary objective of the IO Program is to ensure that units and staff organizations conducting intelligence activities do not infringe on or violate the rights of US persons. However, it is important to note that the program applies to all intelligence activities whether they deal with US

person information or not. Commanders, inspectors general, and judge advocates at all levels need to be cognizant of IO policies and requirements.

2. Conduct of Intelligence Activities. Information concerning capabilities, intentions, and activities of foreign governments and non-state actors is essential in decision-making for national defense and foreign relations. The measures used to acquire such information must be responsive to the legitimate needs of the US Government, and must be in compliance with the constitutional rights and privileges of US persons and IAW with DoD 5240.1-R and other applicable regulations.

2.1. This instruction directs all Air Force personnel potentially working with data collected on US persons to be knowledgeable of, and adhere to, the restrictions and procedures in DoD 5240.1-R, (see Index at Attachment 2, Training Program Primer).

2.2. This instruction neither authorizes any activity not previously authorized nor exempts anyone from any restrictions in DoD 5240.1-R.

3. Scope.

3.1. This instruction applies to all Air Force active duty, Air Force Reserve Command, and Air National Guard (when performing a federal function) intelligence units, staff organizations, and non-intelligence organizations that perform intelligence-related activities (e.g., Eagle Vision units) that could collect, analyze, process, retain, or disseminate information on US persons and it also applies to those who exercise command over these units and organizations. It applies to all military and civilian personnel, to include Host Nation employees, assigned or attached to those units on a permanent or temporary basis, regardless of specialty or job function. Also, it applies to contractors or consultants if they are involved in activities subject to the procedures in DoD 5240.1-R. For Air Force Reserve Command, this AFI applies to Traditional Reservists, Air Reserve Technicians, Individual Mobilization Augmentees, and other Air Force Reserve Command members assigned or attached to intelligence units and staffs or performing intelligence-related activities. For the Air National Guard (ANG), it applies to all ANG members in a Title 10 or Title 32 status assigned or attached to intelligence units or staffs performing intelligence-related activities. (ANG personnel not in Title 10 or Title 32 status may not perform federal intelligence activities.) Additionally, all personnel with a Core Intelligence AFSC must complete IO training regardless of unit mission, duty title, or assignment.

3.2. This instruction also applies to non-intelligence units and staffs (e.g., Eagle Vision) when they are assigned an intelligence mission and to personnel doing intelligence work as an additional duty, even if those personnel are not assigned or attached to an intelligence unit or staff. The Senior Intelligence Officer of the major command (MAJCOM), field operating agency (FOA), or ANG intelligence unit determines applicability.

3.3. This instruction applies to Air Force units and staffs that conduct information operations which include cyberspace activities and are components of intelligence organizations. It also applies to all intelligence personnel described in paragraph 3.1, who support information operations activities with products or services.

3.4. This instruction applies to non-intelligence units or staffs, such as Eagle Vision, operating systems that acquire and disseminate commercial satellite products to intelligence units and staffs.

3.5. This instruction does not apply to criminal investigations conducted by the Air Force Office of Special Investigations (AFOSI). See Air Force Instruction (AFI) 71-101 Volume 1, *Criminal Investigations.*

4. Responsibilities.

4.1. Inspector General (SAF/IG). Chairs and is a voting member of the Air Force IO Panel. Compiles inputs from SAF/GC, AF/A2, SAF/IGX and MAJCOM/FOA/DRU Inspectors General to provide quarterly and annual reports to the Assistant to the Secretary of Defense, Intelligence Oversight ATSD (IO) as specified in paragraph 7. Has access to all material necessary to perform assigned IO responsibilities.

4.2. Secretary of the Air Force, General Counsel (SAF/GC). Legal counsel for Air Force IO issues. Provides legal opinions and advice to intelligence components in coordination with the servicing legal office responsible for advising the intelligence component on questions of legality or propriety, as required. Voting member of the IO Panel. Provides input to SAF/IG in preparation of quarterly reports to the ATSD (IO) as specified in paragraph 7. Has access to all material necessary to perform legal and IO responsibilities.

4.3. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2). Develops guidance to ensure the proper supervision and control of Air Force intelligence activities. Coordinates with the ATSD(IO), the SAF/IG, and the SAF/GC on IO matters. Voting member of the IO Panel. Shall perform annual self-inspection, if necessary, per paragraph 6.2. Provides input to SAF/IG in preparation of quarterly reports to the ATSD(IO) as specified in paragraph 7. Ensures all units directly reporting to or supporting Air Staff (AF/A2) comply with both the provisions of this instruction and those contained in all appropriate intelligence discipline-specific instructions.

4.4. Judge Advocate General (AF/JA). Provides functional oversight to legal offices responsible for advising the DoD intelligence components. Voting member of the Intelligence Oversight Panel. Responsible for OI training of judge advocates, civilian attorneys, and paralegals with intelligence activity responsibilities. In conjunction with SAF/GC, reviews intelligence related policy directives, regulations, and training policies.

4.5. MAJCOMs, FOAs, and Direct Reporting Units (DRUs) that perform Intelligence Activities, as defined in paragraph 3. Establish and maintain IO programs that effect IO and ensure all personnel assigned or attached to their intelligence components receive training according to paragraph 5. Through their inspector general function, accomplish IO inspections required by AFI 90-201, *Inspector General Activities*. Through their functional staffs, accomplish Staff Assistance Visits (SAV) as determined appropriate by the MAJCOM, DRU, or FOA commander. **Note:** IO inspections of ANG intelligence units and staffs will normally be conducted by the gaining command. However, they may also be inspected by the National Guard Bureau Inspector General when gaining command inspection resources are insufficient or unavailable.

4.6. Air Force Office of Special Investigations (AFOSI). Ensure subordinate AFOSI units comply with both the provisions of this instruction and those contained in all counterintelligence discipline-specific instructions.

4.7. Commanders/Directors of units that perform intelligence activities as defined in Paragraph 3.

4.7.1. Be cognizant of IO procedures.

4.7.2. Ensure that IO rules and regulations are followed by intelligence personnel, and personnel performing intelligence functions.

4.7.3. Levy tasks and missions IAW IO principles.

4.7.4. Designate primary and alternate IO monitors in writing.

4.7.5. Ensure IO training, as specified in paragraph 5 and Attachment 2, is conducted.

4.7.6. Ensure IO reporting, as directed in paragraph 7, is completed.

4.7.7. Senior leadership that command Intelligence or Information Operations units (to include Operations Group Intelligence) must complete initial and annual IO refresher training.

4.8. IO Monitors.

4.8.1. Implement an IO training program, conduct IO training as directed in paragraph 5. and maintain records of this training.

4.8.2. Ensure copies of Executive Order 12333, DoDD 5240.1, DoD 5240.1-R; DoDD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight;* and this instruction are available to the unit in hard or electronic copy.

4.8.3. Perform a self-inspection in the final quarter of the calendar year, as directed by paragraph 6.

4.8.4. Provide assistance in rendering collectability determinations on information acquired about US persons within 90 days, as detailed in paragraph 11.2. If necessary, seek assistance from AF/A2.

4.9. Intelligence Personnel.

4.9.1. Know the mission of your organization.

4.9.2. Be familiar with DoD 5240.1-R, Procedures 1-4, 14 and 15, this instruction, and any organization-specific instructions concerning IO.

4.9.3. Complete initial IO training within 45 days of assignment/employment, pre-deployment training as needed and annual refresher training as detailed in Paragraph 5.

4.10. Inspectors General responsible for units that perform intelligence activities, as defined in Paragraph 3.

4.10.1. Know what intelligence units and/or non-intelligence units perform intelligence activities fall under your Commander's authorities.

4.10.2. Understand IG responsibilities, as highlighted in DoD 5240.1-R, Procedures 14 and 15.

4.10.3. Obtain the necessary clearances to perform the mission.

4.10.4. Understand the mission of those organizations under your jurisdiction and those procedures of DoD 5240.1-R that relate to those missions.

4.10.5. Ensure organizations that perform intelligence functions have an established mechanism for reporting questionable activities.

4.10.6. Report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters, as required, to the Attorney General as provided in paragraph 7.1.

4.10.7. Submit quarterly reports as detailed in paragraph 7.3.

4.10.8. Ensure you have taken the unit's IO training within 45 days of assignment/employment.

4.11. Staff Judge Advocates/Legal Advisors responsible for units that perform intelligence activities, as defined in paragraph 3.

4.11.1. Know what intelligence units and/or non-intelligence units perform activities fall under your Commander's authorities.

4.11.2. Understand the legal responsibilities as highlighted in DoD 5240.1-R, Procedures 14 and 15.

4.11.3. Obtain the necessary clearances in order to provide legal advice on IO issues.

4.11.4. Understand the missions of the organizations under your jurisdiction and the procedures of DoD 5240.1-R that relate to those missions.

4.11.5. Complete initial IO training within 45 days of assignment/employment, pre-deployment training if needed and annual refresher training as detailed in Paragraph 5.

4.11.6. Report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters, as required, to the Attorney General as provided in paragraph 7.1.

5. Training.

5.1. **Initial Training.** Technical training centers will ensure initial IO training completion for all Air Force intelligence personnel as part of their technical training. IO monitors will ensure training is provided to all personnel identified in paragraph 3 within 45 days of arrival to their newly assigned units, to include permanent change of station. IO monitors will also provide initial training to all staff judge advocates and inspectors general within 45 days of employment or assignment. Training will include, at a minimum, the matters set out in Attachment 2.

5.2. **Annual Refresher Training.** IO monitors will provide annual refresher training to all Air Force personnel and other personnel identified in paragraph 3, who are assigned or attached to, or employed by, Air Force intelligence components. This training will include, at a minimum, the matters set out in Attachment 2. Units will keep records of personnel training. Annual Refresher training at minimum will be accomplished by completion of the AF/A2 standardized IO computer based training (CBT) module which is hosted on the ADLS website: **https://golearn.csd.disa.mil/kc/login/login.asp**. Use of the CBT as the training standard for initial, annual, and pre-deployment training is mandatory as of 1 August 2010. IO Monitors are encouraged to provide additional training tailored to unit mission. Units will utilize the ADLS system to maintain records of personnel training. Additional information is available on the AF IO Page at: .

5.3. **Pre-Deployment Training.** IO monitors will ensure deploying personnel will retain currency for the duration of the deployment or temporary duty (TDY). If currency will lapse during the deployment or TDY, refresher training must be completed to fulfill the annual training requirement prior to departure.

5.4. AF/A2 has developed a standardized IO computer based training (CBT) module which will be hosted by the Advanced Distributed Learning Service (ADLS) at the following website: . Use of the CBT as the training standard for initial, annual, and pre-deployment training is mandatory as of 1 August 2010. IO Monitors are encouraged to provide additional training tailored to unit mission.

6. Program Inspection Guidance. SAV team members and units will follow the guidance in Attachment 3. Inspectors will assess the unit's and/or staff's compliance with the rules and procedures pertaining to collecting, retaining, and disseminating intelligence on US persons and the adequacy of IO programs. Refer to AFI 90-201 for Inspector General compliance inspection requirements.

6.1. Functional representatives shall use Attachment 3 when accomplishing compliance-oriented SAVs.

6.2. Intelligence units shall perform a self-inspection, using the checklist in Attachment 3, in the final quarter of each calendar year. A self-inspection will be conducted by all units, to include units which were evaluated by ATSD(IO), MAJCOM, FOA, or DRU Inspectors General, or functional staffs accomplishing compliance oriented SAVs. The results shall be forwarded to MAJCOM, FOA, or DRU inspector general. Results of ANG inspections will also be provided to the National Guard Bureau Inspector General.

7. Identifying, Investigating and Reporting Questional Activities.

7.1. **Reporting Questionable Intelligence Activities and Highly Sensitive Matters.** Air Force agencies, units, and personnel must report any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, or applicable DoD policy, including DoD 5240.1-R, this instruction, and/or other Air Force policy documents and instructions. Such a violation is not a "questionable activity" in this context unless there is some nexus between the activity and an intelligence function. SAF/GCM, in coordination with the servicing legal office or supervisory JA chain, can provide assistance in making such determinations. DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities Significant or Highly Sensitive Matters*, Attachment 2, provides reporting parameters and submission procedures. These reports must be filed immediately.

7.1.1. Air Force agencies, units, and personnel must report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters, and crimes to SAF/GC, SAF/IG, AF/JA, AF/A2, the DoD General Counsel or ATSD(IO) using the supervisory chain of command when feasible. Such reports will be expeditiously provided to the inspector general at the first level at which an Inspector General is assigned and not associated with the questionable activity, with copies to the Staff Judge Advocate and, unless the Inspector General determines such reporting would not be appropriate, to senior intelligence officers at the same level. This report must be made regardless of whether a criminal or other investigation has been initiated.

7.1.2. MAJCOMs/FOAs/DRUs similarly will report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters and crimes to SAF/IG through their Inspectors General, providing information copies of the report to SAF/GC and AF/A2.

7.1.3. SAF/IG, SAF/GC, and AF/A2 will immediately report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters, as required, to the Attorney General, the DoD General Counsel and the ATSD(IO). Any such reports, and the quarterly reports described in paragraph 7.3 are exempt from Report Control Symbol (RCS) licensing procedures according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections.*

7.2. **Identifying, Investigating and Reporting Questionable Activities.** Commanders will investigate any questionable activity reported under paragraph 7.1., to the extent necessary to determine whether the reported activity violates law, executive order, Presidential directive, DoD directive or policy, or Air Force instruction or policy. Investigations will be conducted as quickly as possible and the results forwarded through command channels to SAF/IG. Officials responsible for investigations may obtain additional assistance from within the component concerned or from other DoD components, when necessary, to complete investigations in a timely manner. SAF/IG and SAF/GC must have all information necessary to evaluate the questionable activity for compliance with law or policy, regardless of classification or compartmentation.

7.3. **Submitting Annual and Quarterly IO Reports.**

7.3.1. AF/A2 must submit annual and quarterly IO reports to SAF/IGI. Annual reports will be a roll-up of previous quarterly reports. Inputs for the quarterly reports are due to SAF/IGI two calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a single AF report, coordinate with SAF/IG, SAF/GC, AF/JA and AF/A2, and provide to ATSD(IO). Inputs must include:

7.3.1.1. A summary of any substantive Air Force-level change(s) to IO programs, including changes to supporting training programs, and the reason(s) for the change(s). Attach a copy of the directive or policy directing the change.

7.3.1.2. A summary of any Air Force-level changes to published directives or policies concerning intelligence, or intelligence-related activities and the reason for the changes. Attach a copy of the directive or policy directing the change.

7.3.1.3. A description of any intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as any actions taken as a result of the violations.

7.3.1.4. The status of any ongoing Procedure 15 investigations and additional matters pertinent to the Air Force IO programs.

7.3.2. Each MAJCOM, FOA, or DRU Inspector General responsible for an Air Force organization or staff subject to this instruction must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI two calendar days after the end of each quarter. SAF/IGI will

consolidate all inputs into a single AF report, coordinate with SAF/IG, SAF/GC, AF/JA and AF/A2, and provide to ATSD(IO). Inputs must include:

7.3.2.1. A description of any verified Questionable Intelligence Activity and/or Significant or Highly Sensitive Matters will be reported, as required, to the Attorney General as provided in paragraph 7.1. (not confined to US persons-associated violations) identified during the quarter and reference to any report previously made concerning them (see paragraph 7.1.).

7.3.2.2. A description of corrective actions taken regarding questionable activities.

7.3.2.3. A list of IO evaluations or inspections by unit and location and a summary of the results or trends. Include any questionable activity discovered, the familiarity of personnel with IO requirements, and the adequacy of organization IO programs, structure, and processes. Include results of inspections conducted by any outside agency such as ATSD(IO) (include unit and location), and planned next-quarter IO inspections (provide unit and location). If any evaluations or inspections reveal deficiencies, note the corrective action(s) taken.

7.3.2.4. The status of self-inspections conducted IAW paragraph 6 will be attached to the IO report for the last quarter of each calendar year.

7.3.2.5. The MAJCOM, FOA or DRU report for the last quarter of each calendar year will include a list of the units and staffs for which they have IO and inspection requirements (specifying MAJCOM, parent organization, unit designation, and location). **Note:** This list may be classified due to the unit's mission. Ensure the report is marked with its appropriate classification and handled accordingly. Classified packages must follow proper classification guidelines in IAW DoD 5200.1-R, *Information Security Program Regulation* and AFI 31-401, *Information Security Program Management*. SCI packages must follow the appropriate guidelines provided in DoD 5105.21-M-1, *Department of Defense Sensitive Compartmented Information Administrative Security Manual,* and Intelligncе Community Directive 710, *Classification and Control Markings System*.

7.3.2.6. Significant oversight activities undertaken during the quarter and any suggestions to improve the IO program.

8. The IO Panel consists of SAF/IG (chair), SAF/GC, AF/A2 and AF/JA. It reviews the legality and propriety of Air Force intelligence activities, the adequacy of guidance for Air Force intelligence unit and staff IO programs and the state of IO activities, etc.

9. Domestic Imagery. Air Force components may, at times, require newly collected or archived domestic imagery to perform certain missions. Domestic imagery is defined as any imagery collected by satellite (national or commercial) and airborne platforms that cover the land areas of the 50 United States, the District of Columbia, and the territories and possessions of the US, to a 12 nautical mile seaward limit of these land areas.

9.1. Collecting information on specific targets inside the US raises policy and legal concerns that require careful consideration, analysis and coordination with legal counsel. Therefore, Air Force components should use domestic imagery only when there is a justifiable need to do so, and then only IAW EO 12333, the National Security Act of 1947, as amended, DoD

5240.1-R, and this instruction. The following generally constitute legally valid requirements for domestic imagery:

9.1.1. Natural Disasters. Locations in support of government planning for, emergency response to, or recovery from events such as tornadoes, hurricanes, floods, mudslides, fires, and other natural disasters.

9.1.2. Counterintelligence, Force Protection, and Security-related Vulnerability Assessments. Requirements in support of critical infrastructure analysis on federal or private property where consent has been obtained as appropriate.

9.1.3. Environmental Studies. Requirements in support of studies of wildlife, geologic features, or forestation, or similar scientific, agricultural, or environmental studies not related to regulatory or law enforcement actions.

9.1.4. Exercise, Training, Testing, or Navigational Purposes. Requirements for imagery coverage in support of system or satellite calibration, sensor evaluation, algorithm or analytical developments and training or weapon systems development or training..

9.2. **Domestic Imagery from National Satellites.** The National Geospatial-Intelligence Agency (NGA) is responsible for the legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites. Air Force components must follow policy and procedures established in the National System for Geospatial Intelligence Manuals CS 9400.07, *Domestic Imagery.* Air Force components must submit a PUM each year to NGA that defines the requirements for domestic imagery, outlines its intended use, and includes a proper use statement acknowledging awareness of legal and policy restrictions regarding domestic imagery. NGA will review the PUM to ensure it constitutes a legally valid requirement for domestic imagery. Air Force components must submit a Domestic Imagery Request (DIRs) to NGA for any ad hoc domestic imagery requirements that fall outside the scope of an approved PUM.

9.3. **Domestic Imagery from all DoD imagery Satellite Platforms.** An approved PUM must be on file with the appropriate Combatant Command, per their procedures, or with the appropriate Air Force MAJCOM or FOA (or delegated/designated sub-component PUM authority) before airborne or tactical DoD satellite platforms can be tasked to collect domestic imagery. Note that Tactical Satellites (TacSats) are considered to be "airborne" platforms. These PUMs must be IAW the format instructions found in Attachment 4. Approval for PUM requests is hereby delegated to MAJCOM and FOA commanders. Legal review at MAJCOM/FOA level is required before approval and reviews should be filed with the approved PUM requests. In the event of an emergency or crisis where US Northern Command (USNORTHCOM) is designated as lead DoD Operational Authority, all related requests for domestic imagery from airborne or tactical DoD satellite platforms must be coordinated with USNORTHCOM to ensure compliance with proper use provisions. Air Force components must submit a PUM request through the MAJCOM to the designated approval authority for any ad hoc DIR. (see paragraph 9.6. for an exception to this paragraph).

9.4. **Domestic Imagery from Commercial Satellites.** Air Force intelligence components may obtain domestic commercial imagery without higher-level approval for valid mission purposes such as training or testing on federally owned and operated ranges, calibration-

associated systems development activities, and domestic disaster relief operations. However, an internal memorandum for record (MFR) describing the purpose of the domestic imagery and the component official approving the use should be retained on file. If obtained imagery specifically identifies a US person (include private property), then the rules and procedures contained in DoD 5240-1.R, in particular those regarding retention, must be followed. Air Force intelligence components must not conduct or give the appearance ofconducting collection, exploitation or dissemination of commercial imagery or imagery associated products for other than approved mission purposes.

9.5. **Distribution of Domestic Imagery.** Distribution of domestic imagery to parties other than those identified in the approved PUM, DIR or MFR is prohibited, unless the recipient is reasonably perceived to have a specific, lawful governmental function requiring it IAW paragraph 11.4. Unless otherwise approved, domestic imagery must be withheld from all general access database systems (e.g., Intelink).

9.6. **Navigational/Target Training activities.**

9.6.1. Air Force units with weapon system video and tactical ISR capabilities may collect imagery during formal and continuation training missions as long as the collected imagery is not for the purpose of obtaining information about specific US persons or private property. Collected imagery may incidentally include US persons or private property without consent. Imagery may not be collected for the purpose of gathering any specific information about a US person or private entity, without consent, nor may stored imagery be retrievable by reference to US person identifiers.

9.6.2. Air Force Unmanned Aircraft System (UAS) operations, exercise and training missions will not conduct nonconsensual surveillance on specifically identified US persons, unless expressly approved by the Secretary of Defense, consistent with US law and regulations. Civil law enforcement agencies, such as the US Customs and Border Patrol (CBP), Federal Bureau of Investigations (FBI), US Immigration and Customs Enforcement (ICE), and the US Coast Guard, will control any such data collected.

10. Force Protection.

10.1. AFI 14-119, *Intelligence Support to Force Protection (FP)*, stipulates that intelligence personnel at all levels will work in coordination with their cross-functional counterparts (e.g., AFOSI, SF, ATOs, etc.) to ensure FP threat/intelligence requirements are satisfied. If during the course of routine, non-force protection related, intelligence activities and authorized missions, Air Force intelligence components receive information identifying US persons as an alleged threat to DoD or civilian individuals, entities or structures, such threats should be reported IAW paragraph 12 of this instruction.

10.2. Air Force intelligence assets assigned a mission to support force protection activities by a governmental entity that has responsibility for countering the threat may assist in fusing law enforcement and counterintelligence, with intelligence information in support of force protection (e.g., antiterrorism and/or law enforcement activities), consistent with IO procedures. AFI 14-119 provides guidance to support force protection mission execution.

11. Procedural Guidance. Air Force intelligence components may only engage in activities involving the deliberate collection of information about US persons under the procedures set forth in DoD 5240.1-R and this instruction.

11.1. **General.** Any collection, retention and/or dissemination of US person information must be based on a proper function/mission assigned to the component and must follow the guidance in DoD 5240.1-R and this instruction.

11.2. **Collection.** Information about US persons may be collected if it falls within one or more of the thirteen categories of information specified in DoD 5240.1-R, Procedure 2.

11.2.1. Information is considered "collected" only when it has been received for use by an employee of an intelligence component in the course of official duties. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

11.2.2. Temporary Retention. Information inadvertently received about US persons may be kept temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be collected under the provisions of Procedure 2, DoD 5240.1-R and permanently retained under the provisions of Procedure 3, DoD 5240.1-R. If there is any doubt as to whether the US person information may be collected and permanently retained, the receiving unit should seek advice through the chain of command, Judge Advocate General (JAG), or IO monitor. The unit/MAJCOM IO Monitor must provide assistance in rendering collectability determinations. When appropriate, assistance may be requested from AF/A2. A determination on whether information is collectible must be made within 90 days.

11.2.2.1. If a determination is made that information is not properly collectible before the expiration of the 90 day period, it must be purged or transferred immediately.

11.2.2.2. Even though information may not be collectible, it may be retained for the length of time necessary to transfer it to another DoD entity or government agency to whose function it pertains.

11.2.3. Means of Collection. When Air Force intelligence components are authorized to collect information about US persons, they may do so by any lawful means, subject to the following limitations.

11.2.3.1. Least Intrusive Means. Collection of information about US persons shall be accomplished by the least intrusive means. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought.

11.2.3.2. Foreign Intelligence Collection Within the United States. Within the US, foreign intelligence concerning United States persons may be collected only by overt means except as provided below. Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that the information is being provided to the DoD, or a component thereof:

11.2.3.2.1. The foreign intelligence sought must be significant and not being collected for the purpose of acquiring information concerning the domestic activities of any US person;

11.2.3.2.2. The foreign intelligence cannot reasonably be obtained by overt means;

11.2.3.2.3. The collection of such foreign intelligence has been coordinated with the FBI;

11.2.3.2.4. The use of other than overt means has been approved by the Secretary of the Air Force. Authority to approve such requests is hereby delegated to the AF/A2. AF/A2 will provide a copy of any such approval to the Undersecretary of Defense for Intelligence (USD(I));

11.3. **Retention.** Retention limitations apply to information about US persons that is knowingly retained without the consent of the person whom the information concerns. These limitations do not apply to information retained solely for administrative purposes or is required by law to be maintained. "Retention" refers only to the maintenance of information about US persons that can be retrieved by reference to the person's name or other identifying data.

11.3.1. US person information that is properly collected and retained will be reviewed periodically to ensure that continued retention serves the purpose for which it was collected and stored, and that retention remains necessary to the conduct of authorized functions of the Air Force intelligence component concerned.

11.4. **Dissemination.** US person information in the possession of an Air Force intelligence component may be disseminated pursuant to law, a court order, or IAW the following criteria:

11.4.1. The information was properly collected or retained or both under Procdures 2 and 3 of DoD 5240.1-R.

11.4.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function and is:

11.4.2.1. An employee of the DoD or an employee of a contractor of the DoD who has a need for such information in the course of their official duties.

11.4.2.2. A law enforcement entity of federal, state or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce.

11.4.2.3. An agency within the intelligence community. Whether the information is relevant to the responsibilities of any such intelligence agency is a determination to be made by the agency concerned.

11.4.2.4. An agency of the federal government authorized to receive such information in their performance of a lawful governmental function.

11.4.2.5. A foreign government and dissemination is undertaken pursuant to an agreement or other understanding with such government.

11.5. **Electronic Surveillance.**

11.5.1. Electronic surveillance, for counterintelligence purposes must be conducted IAW instructions and procedures promulgated by the Commander, AFOSI, approved by the Secretary of the Air Force, and contained in Signals Intelligence (SIGINT) directives, including United States Signals Intelligence Directive (USSID) SP0018.

11.5.2. Requests to perform electronic surveillance, to include computer network exploitation, for foreign intelligence collection or against US persons abroad for foreign intelligence purposes, whether consensual or nonconsensual, must be forwarded to the AF/A2 for approval. AF/A2 will coordinate with SAF/GCM.

11.6. **Concealed Monitoring.** Monitoring of individuals within the US or US persons outside the United States, where the subject of such monitoring does not have a reasonable expectation of privacy and no warrant would be required if the monitoring were undertaken for law enforcement purposes, requires the approval of the Commander, AFOSI after consultation with AFOSI/JA (for counterintelligence) or the AF/A2 after consultation with SAF/GCM (foreign intelligence).

11.6.1. Approval officials must determine that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions and does not constitute electronic surveillance.

11.6.2. Within the US, an Air Force intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by DoD or otherwise in the course of an investigation conducted for counterintelligence purposes pursuant to the *Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation,* dated 5 April 1979.

11.6.3. Outside the US, concealed monitoring may be conducted on installations and facilities owned, or otherwise lawfully occupied by the DoD. Monitoring outside such facilities shall only be conducted after coordination with appropriate host country officials, if such coordination is required by the governing status of forces agreement (SOFA), and with the Central Intelligence Agency (CIA).

11.7. **Physical Searches.** A physical search is any intrusion upon a person or a person's property or possessions to obtain items of property or information. Examination of areas that are in plain view and visible to the naked eye if no physical trespass is required, or of items that are abandoned in a public place, does not constitute a physical search. Any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to DoDD 5240.1, Procedure 5, Parts 1 and 2, does not constitute a physical search.

11.7.1. Physical Searches within the United States. AFOSI is authorized to conduct nonconsensual searches in the US for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military judge or magistrate, or a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers. Air Force intelligence components may not otherwise conduct nonconsensual physical searches within the US for foreign intelligence or counterintelligence purposes.

11.7.2. Physical Searches outside the United States.

11.7.2.1. AFOSI may conduct nonconsensual physical searches for counterintelligence purposes of persons or property of active duty military personnel outside the US when authorized by a military judge or magistrate, or a commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe such persons are acting as agents of foreign powers.

11.7.2.2. For foreign intelligence or CI purposes, other non-consensual physical searches of the person or property of US persons, may be conducted only pursuant to the approval of the Attorney General.

11.7.2.3. Within a commander's Status of Forces Agreement (SOFA) authorities, nonconsensual physical searches of non-US persons abroad must be IAW any applicable SOFA and approved by the Installation Commander. Nonconsensual physical searches of non-US persons abroad may be approved by the Commander, AFOSI for counterintelligence purposes and by the AF/A2 for foreign intelligence purposes.

11.8. **Searches and Examination of Mail.**

11.8.1. Applicable postal regulations do not permit the Air Force to detain or open first class mail within US postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service. Searches of first class mail in US military postal channels overseas may only be authorized under procedures established in DoD 4525.6-M, *Department of Defense Postal Manual*, Chapter 10.

11.8.2. Air Force intelligence components may request that appropriate US postal authorities inspect, or authorize the inspection of second, third or fourth class mail in US postal channels IAW applicable postal regulations. Such components may also request that US postal authorities detain, or permit detention of, mail that may become subject to search under applicable postal regulations.

11.8.3. Air Force intelligence components may open mail to or from a US person that is found outside US postal channels only with the approval of the Attorney General. Any requests for such authorization for foreign intelligence purposes will be forwarded through the AF/A2, and for counterintelligence purposes through the Commander, AFOSI.

11.8.4. Mail outside US postal channels when both the sender and intended recipient are other than US persons, may be searched if such search is otherwise lawful and consistent with any applicable SOFA. For counterintelligence purposes, such searches must be approved by the Commander, AFOSI, and for foreign intelligence purposes, by the AF/A2.

11.8.5. Mail Covers. The Commander, AFOSI may request US postal authorities examine mail in US postal channels for counterintelligence purposes, IAW postal regulations. The Commander, AFOSI may also request mail covers from appropriate foreign officials, with respect to mail to or from a US person that is outside US postal

channels, IAW appropriate law and procedures of the host government and any SOFA that may be in effect.

11.9. **Physical Surveillance.** Physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. Any physical surveillance that occurs outside a DoD installation shall be coordinated with the FBI (within the US), CIA (outside the US), or other agency as appropriate.

11.9.1. Physical surveillance for counterintelligence purposes, both within and outside the US, shall be approved and conducted IAW DoD 5240.1-R and procedures established by the Commander, AFOSI.

11.9.2. Physical surveillance for foreign intelligence purposes shall be approved and conducted IAW DoD 5240.1-R and procedures established by the AF/A2, or his/her designee.

11.10. **Undisclosed Participation in Organizations.** Participation by an employee of an Air Force intelligence component, on behalf of an intelligence component, in any organization within the US or any organization outside the US that constitutes a US person, must be approved IAW the requirements in subparagraphs 11.10.1. and 11.10.2. Undisclosed participation that occurs outside a DoD installation must be coordinated with the FBI (within the US), through the AFOSI, CIA (outside the US), or other agency as required. Intelligence component employees do not require permission to participate in organizations for solely personal purposes.

11.10.1. Undisclosed participation, for counterintelligence purposes, must be approved and conducted IAW procedures approved by the Commander, AFOSI, and, DoD 5240.1-R.

11.10.2. Undisclosed participation by personnel assigned to the AF ISR Agency for foreign intelligence purposes must be approved by Commander, AFISRA, or his designee and conducted 747 according to DoD 5240.1-R.

11.10.3. Outside AFISRA, undisclosed participation for foreign intelligence purposes must be approved by AF/A2, or its delegate, and IAW DoD 5240.1-R and procedures established by AF/A2.

11.11. **Contracting for Goods and Services.** DoD 5240.1-R, Procedure 11 applies to contracting or other arrangements with US persons for the procurement of goods and services by or for an Air Force intelligence component within the US. It does not apply to contracting with government entities, or to the enrollment of individual intelligence personnel as students with academic institutions. When non-disclosure of intelligence component sponsorship is necessary in contracts for enrollment of students in academic institutions, the provisions of paragraph 11.10 apply.

11.11.1. Cooperation with law enforcement authorities. Subject to the limitations of this Instruction, Air Force intelligence components may cooperate with law enforcement authorities IAW DoDD 5525.5, DoD Cooperation with Civilian Law Enforcement Officials, for the purpose of:

11.11.1.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, incident to approved activities; or

11.11.1.2. There is a written determination by the Secretary or Under Secretary of the Air Force that the sponsorship by an Air Force intelligence component must be concealed to protect the activities of the intelligence component concerned. This authority may not be delegated.

11.12. **Assistance to Law Enforcement.**

11.12.1. Cooperation with law enforcement authorities. Subject to the limitations outlined in paragraph 11.12.2. of this Instruction, Air Force intelligence components may cooperate with law enforcement authorities IAW DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials,* for the purpose of:

11.12.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

11.12.1.2. Protecting DoD employees, information, property and facilities;

11.12.1.3. Preventing, detecting, or investigating other violations of law.

11.12.2. Types of permissible assistance. Air Force intelligence components may only provide the types of assistance to law enforcement authorities delineated below. Assistance may not be provided for, or participation in, activities that would not be permitted under this instruction.

11.12.2.1. Violations of US federal law. Incidentally acquired information reasonably believed to indicate a violation of federal law shall be provided to appropriate federal law enforcement officials through AFOSI channels.

11.12.2.2. Other violations of law. Information incidentally acquired during the course of Air Force counterintelligence activities reasonably believed to indicate a violation of state, local, or foreign law will be provided to appropriate officials IAW procedures established by the Commander, AFOSI. Information incidentally acquired during the course of Air Force foreign intelligence activities reasonably believed to indicate a violation of state, local, or foreign law will, unless otherwise decided by AF/A2 for national security reasons, be provided to AFOSI IAW procedures established by the AF/A2, or his/her designee, for investigation or referral to the appropriate law enforcement agency. Information covered by this paragraph includes US person information (See paragraph 12.).

11.12.2.3. Provision of specialized equipment and facilities. Specialized intelligence equipment and facilities may be provided to federal law enforcement authorities, and, when lives are endangered, to state and local law enforcement authorities, only with the approval of the SecAF delegated authority and the concurrence of SAF/GC.

11.12.2.4. Assistance of Air Force intelligence personnel. Air Force intelligence personnel may be assigned to assist federal law enforcement authorities with the approval of the SecAF delegated authorityand the concurrence of SAF/GC. Under certain exigent circumstances (e.g., when lives are in danger), Air Force intelligence

personnel may be assigned to assist state and local law enforcement authorities, provided such assistance has been approved by the Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services (AF/A1) and SAF/GC.

11.13. **Experimentation on Human Subjects for Intelligence Purposes.** Air Force intelligence components do not engage in experimentation involving human subjects for intelligence purposes. Any exception would require approval by the Secretary or Under Secretary of the Air Force and would be undertaken only with the informed consent of the subject and IAW procedures established by AF/SG to safeguard the welfare of subjects.

11.13.1. Experimentation means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

11.13.2. Experimentation is conducted on behalf of an Air Force intelligence component if it is conducted under contract to Air Force or to another DoD component for the benefit of the Air Force or at the request of the Air Force regardless of the existence of a contractual relationship.

11.13.3. For purposes of this instruction, the term "human subjects" includes any person, whether or not such person is a US person. No prisoners of war, civilian internees, retained, and detained personnel as covered under the Geneva Conventions of 1949 may be the subjects of human experimentation.

12. Reporting of Incidentally Acquired Threat Information. If, during the course of routine activities and authorized missions, Air Force intelligence components receive information (including information identifying US persons) regarding potential threats to life or property, (whether DoD personnel, installations or activities, or civilian lives or property) that information must be passed to appropriate authorities.

12.1. In the event that the threat information involves an imminent threat to life or serious property damage, the Air Force intelligence component will immediately notify appropriate entities with responsibility for countering the threat (e.g., Base Command Section, Security Forces, FBI, Municipal Police Department, etc.). The Air Force intelligence component must also immediately notify AFOSI. In the event immediate notification of the local AFOSI unit is not possible, the Air Force intelligence component will notify the AFOSI Global Watch Center, DSN 857-0393, Commercial 240-857-0393, or Commercial Toll Free 1-877-246-1453.

12.1.1. Absent imminent threat, reporting should be limited to AFOSI who will determine whether further reporting will unacceptably compromise potential investigative or operational activities and forward to other authorities as appropriate.

12.1.2. Threat information may only be withheld from dissemination upon the approval of AF/A2 for foreign intelligence or Commander, AFOSI for counterintelligence, and only for national security reasons.

13. The Internet. While much of the information posted on the Internet is publicly available, Air Force intelligence components must have an official mission requiring it before collecting,

retaining, or disseminating even publicly available information about US persons. Certain internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation. This also applies to information found on SIPRNET and JWICS.

LARRY D. JAMES, Lt Gen, USAF
Deputy Chief of Staff, Intelligence Surveillance and Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, 2 April 2004

AFI 10-801, *Assistance to Civilian Law Enforcement Agencies*, 15 April 1994

AFI 14-119, *Intelligence Support to Force Protection (FP)*, 15 August 2007

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

AFI 90-201, *Inspector General Activities*, 17 June 2009

AFMAN 33-363, *Management of Records*, 1 March 2008

Executive Order Number 12333, *United States Intelligence Activities*, December 4, 1981

National Security Act of 1947, 50 United States Code, Sections 401 et sequentia

DoDD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))*, September 20, 2010

DoDD 5240.1, *DoD Intelligence Activities*, August 27, 2007

DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials*, January 15, 1986

DTM 08-052 – *DoD Guidance for Reporting Questionable Intelligence Activities Significant or Highly Sensitive Matters*, June 17, 2009

DoD 4525.6-M, *Department of Defense Postal Manual*, August 15, 2002

DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, December 1, 1982

DoD 4525.6-M, *Department of Defense Postal Manual*, Attachment 1

DoD 5105.21-M-1, *Department of Defense Sensitive Compartmented Information Admisitrative Security Manual*, August 1998

DoD 5200.1-R, *Information Security Program Regulation*, January 14, 1997

United States Signals Intelligence Directive (USSID) SP0018, 27 July 1993

National System for Geospatial Intelligence Manual CS 9400.07, *Domestic Imagery*, Revision 5, March 2009

Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979

Intellignce Community Directive 710, *Classification and Control Markings System*, September 11, 2009

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 9 September 2009

Abbreviations and Acronyms

ADLS—Advance Distributed Learning Service

AF/A1—Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services

AF/A2—Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance

AFI—Air Force Instruction

AF ISR Agency—Air Force Intelligence, Surviellance, and Reconnaissance Agency

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AF/SG—Surgeon General

ANG—Air National Guard

ATSD(IO)—Assistant to the Secretary of Defense for Intelligence Oversight

CBP—United States Customs and Border Patrol

CBT—Computer Based Training

CIA—Central Intelligence Agency

CoP—Community of Practice

DIR—Domestic Imagery Request

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

EO—Executive Order

FBI—Federal Bureau of Investigation

FOA—Field Operating Agency

IAW—In Accordance With

ICE—United States Immigration and Customs Enforcement

IG—Inspector General

IO—Intelligence Oversight

ISR—Intelligence, Surveillance, and Reconnaissance

JA—Judge Advocate

JAG—Judge Advocate General

JWICS—Joint Worldwide Intelligence Communication System

MAJCOM—Major Command

MFR—Memorandum For Record

NGA—National Geospatial-Intelligence Agency

NIPRNET—Unclassified but Sensitive (N-level) Internet Protocol Router Network

NSA—National Security Agency

OPR—Office Of Primary Responsibility

PUM—Proper Use Memorandum

UAS—Unmanned Aircraft System

USD(I)—Undersecretary of Defense for Intelligence

USNORTHCOM—United States Northern Command

RDS—Records Disposition Schedule

SAF/GC—Secretary of the Air Force General Counsel

SAF/IG—Secretary of the Air Force Inspector General

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

SIGINT—Signals Intelligence

SIPRNET—Secret Internet Protocol Router Network

SOFA—Status of Forces Agreement

TDY—Temporary Duty

US—United States

USSID—United States Signals Intelligence Directive

UTM—Unit Training Monitor

Terms

Air Force Intelligence Component—All personnel and activities of the organization of the AF Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, counterintelligence units of the Air Force Office of Special Investigations, Air Force Intelligence Analysis Agency, and other organizations, staffs, and offices when used for foreign intelligence or counterintelligence activities to which EO 12333 (part 2) applies.

Computer Network Exploitation—Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE *and network exploitation (Net-E).*"

Counterintelligence—Information gathered and activities conducted to prevent espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Domestic Imagery Request (DIR)—A request for collection, processing, dissemination, exploitation, briefing, or publication of domestic imagery when that need falls outside the scope of an approved PUM and is not a reflection of a change in an organization's mission. It generally reflects ad hoc requirements for domestic imagery.

Electronic Surveillance—Electronic surveillance, as defined at 50 USC 1801(f)(1)-(4), and as conducted by DoD intelligence components targeting US Persons to collect foreign intelligence information under circumstances in which a warrant would be required for law enforcement purposes. Note that this includes, per 50 USC 1801(f)(4), the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication (such as oral communications acquired by hidden microphone, or location information revealed through the use of a transponder or tracker device), under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Experimentation—Any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

Foreign Intelligence—Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

Human Subjects—Any person, whether or not such person is a US person. No prisoners of war, civilian internees, retained, and detained personnel as covered under the Geneva Conventions of 1949 may be the subjects of human experimentation.

Intelligence Activities— Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333. Note that EO 12333 assigns the Services' intelligence components responsibility for: 1, "Collection, production, dissemination of military and military related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking;" and 2, "Monitoring of the development, procurement and management of tactical intelligence systems and equipment and conducting related research, development, and test and evaluation activities."

Non-United States Person—A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person. A person or organization outside the United States is presumed not to be a US person, unless specific information to the contrary is obtained. An alien in the United States is presumed not to be a US person, unless specific information to the contrary is obtained.

Overt—Methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that the information is being provided to the DoD, or a component thereof.

Physical Surveillance—A systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person who is neither a party thereto nor visibly present thereat, through any means not involving electronic surveillance.

Proper Use Memorandum—A memorandum signed annually by an organization's Certifying Government Official that defines the organization's domestic imagery requirements and intended use. It also contains a proper use statement acknowledging awareness of the legal and policy restrictions regarding domestic imagery.

Questionable Activity—Any intelligence activity, as defined in Executive Order 12333 (Reference (f)), that may be unlawful or contrary to Executive order, Presidential directive, or applicable DoD policy governing that activity.

Retention—The maintenance of information about US persons that can be retrieved by reference to the person's name or other identifying data.

Significant or Highly Sensitive Matters—A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity: (1) Involving congressional inquiries or investigations, (2) That may result in adverse media coverage, (3) That may impact on foreign relations or foreign powers, or (4) Related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations.

United States Person—A US citizen, an alien known by the DoD intelligence component concerned to be a permanent resident alien, an unincorporated association substantially composed of US citizens or permanent resident aliens, or a corporation incorporated in the United States unless it is directed and controlled by a foreign government or governments.

Attachment 2

TRAINING PROGRAM PRIMER

A2.1. Introduction. The material below is provided as a core curriculum for an intelligence unit or staff IO program. It is intended to provide a common sense perspective on this important but often seemingly complex subject.

A2.2. Background. IO has become a commonly understood term referring to a group of laws, directives, and associated institutional bodies designed to ensure that US intelligence activities are conducted legally and properly, and do not infringe on the rights of US persons. For the Air Force, there are two primary governing directives: DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons,* and AFI 14-104, *Oversight of Intelligence Activities*.

A2.3. Tenets. Air Force intelligence personnel should understand the following central tenets of the Air Force IO program:

A2.3.1. Scope. The Air Force IO program pertains to all personnel assigned or attached to intelligence units or staffs that could collect, analyze, process, retain, or disseminate information on US persons. These include active, reserve, guard, civilian, TDY and contractor personnel. See Terms in Attachment 1 for the definition of a US person. Further, the program pertains to any person tasked to perform an intelligence mission regardless of unit of assignment.

A2.3.2. Permissible Activities. Air Force intelligence units and staffs can collect, retain, and disseminate intelligence on US persons only if it is necessary to the conduct of a function or mission assigned to the collecting component and only if it falls within one of the thirteen categories listed under DoD 5240.1-R, Procedure 2. In the US, it is not generally within the mission of military intelligence units to collect information on US persons (this would normally be within the mission of counterintelligence units). As such, although some information on US persons may be "publicly available" (one of the 13 categories referred to above), this does not obviate unit mission/function requirements.

A2.3.3. Collection Techniques. There are very specific procedures and restrictions governing the collection of intelligence on US persons by methods such as electronic surveillance or physical search or through participation in activities of private organizations. (DoD 5240.1-R, Procedures 5-11)

A2.3.4. Law Enforcement Assistance. There are very specific procedures and restrictions on providing intelligence support to law enforcement agencies. (AFI 10-801 *Assistance To Civilian Law Enforcement Agencies*).

A2.3.5. Questionable Intelligence Activities. IO is much broader than just collecting, retaining and disseminating intelligence on US persons. Unit members or staff personnel are required to report "Questionable Intelligence Activities" which is defined as "any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, *United States Intelligence Activities*, or applicable DoD policy, including DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons."* Unit

members or staff personnel are also required to report Significant or Highly Sensitive Matters. (See Atch 1, Terms)

A2.3.6. Reporting. Personnel assigned to intelligence units or staffs must report any possible IO-associated violations or irregularities to the JAG or IO Monitor, the wing or base Inspector General, the Air Force General Counsel, the Air Force Inspector General, or the DoD General Counsel or ATSD(IO). Use the supervisory chain or chain of command to facilitate such reports, where feasible. Such reports will be expeditiously provided to the Inspector General at the first level at which an inspector general is assigned who is not associated with the questionable activity. Copies of the report must be sent to the Staff Judge advocate and, unless the Inspector General determines such reporting would not be appropriate, senior intelligence officers at the same level (DoD 5240.1-R, Procedure 15 and this instruction, paragraph 7.2.).

A2.3.7. The Internet. While much of the information posted on the Internet is publicly available, an intelligence professional acting in an official capacity still must have the official mission before collecting, retaining, or disseminating even publicly available information about US persons. Certain internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation. This also applies to information found on SIPRNET and JWICS (DoD 5240.1-R, Procedure 10 and 11).

A2.4. Reminder. Even though most intelligence personnel are not "collectors," most do retain and disseminate intelligence. Some personnel, such as those working with domestic imagery collection or information warfare programs, may need a more in-depth understanding of select aspects of IO rules and procedures. All are encouraged to periodically check the Air Force IO Community of Practice (CoP) at (NIPRNET:

https://www.intelink.gov/sites/a2z/FormServerTemplates/Intelligence%20Oversight.aspx) as well as the web site maintained by the Assistant to the SECDEF, IO (NIPRNET: **www.DoD.mil/atsdio**; SIPRNET: **www.atsdio.ismc.sgov.gov/atsdio**/; or JWICS: **www.atsdio.ismc.ic.gov/atsdio**/) for soft copies of the basic IO references, additional training aids/software, a list of frequently asked questions/IO examples, and other useful information. Other techniques that can be used to raise awareness are poster campaigns/visual aids and messages posted in newsletters or on bulletin boards.

A2.5. Index - DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that affect United States Persons*

A2.5.1. Procedure 1—General Provisions

A2.5.2. Procedure 2—Collection of Information about US Persons. Note - information that identifies a US person may be collected only if it is necessary to the conduct of a function assigned to the collection component, and only if it falls within one of the categories listed in DoD 5240.1-R, Procedure 2.

A2.5.3. Procedure 3—Retention of Information about US Persons

A2.5.4. Procedure 4—Dissemination of Information about US Persons

A2.5.5. Procedure 5—Electronic Surveillance. Note-this procedure also applies to signals intelligence activities. Refer to the classified annex to EO 12333 and USSID SP0018 for more information.

A2.5.6. Procedure 6—Concealed Monitoring

A2.5.7. Procedure 7—Physical Searches

A2.5.8. Procedure 8—Searches and Examination of Mail

A2.5.9. Procedure 9—Physical Surveillance

A2.5.10. Procedure 10—Undisclosed Participation in Organizations

A2.5.11. Procedure 11—Contracting for Goods and Services Without Revealing the Sponsorship by the Intelligence Component

A2.5.12. Procedure 12—Provision of Assistance to Law Enforcement Authorities

A2.5.13. Procedure 13—Experimentation on Human Subjects for Intelligence Purposes

Note: Procedures 5—13 contain detailed rules, prohibitions, and approval processes for specialized collection methods and techniques. The majority of Air Force intelligence units and staffs will never be required or authorized to conduct the activities described in these procedures, all of which require approval by specific higher level officials. Judge Advocate General or General Counsel authorities should be consulted on any matter pertaining to procedures 5 - 13.

A2.5.14. Procedure 14—Employee Conduct

A2.5.15. Procedure 15—Identifying, Investigating, and Reporting Questionable Activities

Note 1— see discussion of "reporting" above, and in "questionable activities" and "reporting" provisions in this instruction, paragraphs 7.1. and 7.2.

Note 2—Air Force intelligence units and staffs must use the ATSD(IO)-produced IO training program on ADLS as part of the unit or staff IO program.

Note 3—Attachment 3 includes detailed information about individual knowledge of IO necessary to pass an IO inspection and is recommended as a training aid.

Attachment 3

INSPECTION GUIDANCE

This checklist should be used when assessing the adequacy of IO programs. Failure of a critical item requires an "Unsatisfactory" rating for the unit IO program. Results and corrective actions will be reported IAW paragraph 7.3.4.

A3.1. Administrative.

A3.1.1. Ensure the primary and alternate IO monitors are appointed in writing. **Note:** This is a non-critical item. If a unit is not compliant, provide a 10-day answerable action item to the unit to update their paperwork.

A3.1.2. Ensure IO training has been accomplished by all assigned personnel every 12 months, as identified in paragraph 3 and that the records of training are available and current. **Note:** This is a critical item. Failure occurs if more than 25% of unit personnel are not current on their training.

A3.1.3. Ensure initial and annual training lesson plans cover the minimum objectives outlined in Attachment 2. **Note:** This is a non-critical item. If a unit is not compliant, the training lesson plan must be updated within 30 days of the inspection.

A3.1.4. Ensure copies of EO 1233, DoD 5240.1-R, DoDD 5148.11, and this instruction are available to the unit in hard or electronic copy. **Note:** This is a non-critical item. If a unit is not compliant, provide a 10-day action item to the unit to correct the deficiency.

A3.1.5. Ensure units perform a self-inspection, using the checklist in Attachment 3 in the final quarter of each calendar year. Ensure results are forwarded to MAJCOM, FOA, or DRU Inspector General. **Note:** This is a non-critical item. If a unit is not compliant, provide a 10-day action item to the unit to correct the deficiency.

A3.2. Functional.

A3.2.1. Determine if unit members and staff personnel are aware of the applicability of IO limitations to them. **Note:** This item is a critical item. A minimum of 75 % of individuals must be aware of the meaning and limitations for this item to be satisfactory.

A3.2.2. Determine if unit members and staff personnel are aware of the circumstances under which intelligence can be collected, retained, and disseminated on US persons (e.g., information obtained with consent). **Note:** This is a critical item. A minimum of 75% of individuals must be aware that DoD 5240.1-R describes the circumstances under which information on US persons may be collected for this item to be satisfactory. Refer to Attachment 2 and DoD 5240.1-R, Procedure 2 for more details.

A3.2.3. Determine if unit members and staff personnel are aware that there are specific procedures and restrictions governing the collection of intelligence on US persons by methods such as electronic surveillance or physical surveillance. **Note:** This is a critical item. A minimum of 75 % of individuals must be aware of the existence of such limitations and sources of information concerning them for this item to be satisfactory. Refer to Attachment 2, and DoD 5240.1-R, Procedures 5-11 for more details.

A3.2.4. Determine if unit members and staff personnel are aware that there are specific procedures and restrictions on providing intelligence support to law enforcement agencies. **Note:** This is a critical item. A minimum of 75 % of individuals must be aware of the existence of such limitations for this item to be satisfactory. Refer to Attachment 2, and DoD 5240.1-R, Procedure 12 for more details.

A3.2.5. Determine if unit members and staff personnel are aware that they are required to report "questionable activities" conducted by intelligence components that constitute possible violations of law, directive, or policy. Also determine if personnel are aware that using the chain of command for reporting "questionable activities" is encouraged where feasible. **Note:** This is a critical item. A minimum of 75 % of individuals must be aware of the requirement to report "questionable activities" using the chain of command where feasible, for this item to be satisfactory. Refer to paragraph 7.1.1., Attachment 2 in this instruction, and DoD 5240.1-R, paragraph A.2.3.6. and Procedure 15 for more details.

A3.2.6. Determine if unit members and staff personnel understand that "US Person" pertains to associations, corporations, and resident aliens as well as US citizens. **Note:** This is a critical item. A minimum of 75 % of individuals must be aware of the meaning and limitations for this item to be satisfactory. See Attachment 1, Terms for more details.

A.3.2.7. Determine if unit member and staff personnel are aware of AFI 14-104 and DoD 5240.1-R as key IO authorities. Note: This is a non-critical item. Individuals who are not aware will receive remedial training.

Attachment 4

PROPER USE MEMORANDUM (PUM) GUIDANCE FOR AIRBORNE AND DOD SATELLITE PLATFORMS PLATFORMS

A4.1. PUM approval resides with MAJCOM A2 and AFISRA/CC. PUM requests will be submitted to MAJCOM or AFISRA/A2X via fax or email. MAJCOM A2 and AFISRA will coordinate PUM approval with MAJCOM/A2 or AFISRA/JA.

A4.2. PUM requests will include the following information: (1) Units involved (to include units involved in exploitation, (2) Timeframe, (3) Location, (4) Assets being used to conduct collection, and (5) Justification.

A4.3. MAJCOM or AFISRA/A2X will provide a timely response to requesting units that include any rules of engagement, if necessary.